

DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

DoN Systems Design, Engineering, Installation, Operations, Maintenance, Network and Enterprise Engineering Support for CUS

1.0 BACKGROUND

Commander, Undersea Surveillance is a Department of the Navy (DoN) organization that supports global maritime acoustic surveillance and timely, accurate Anti-Submarine Warfare (ASW) reporting using persistent, long-range, fixed and mobile systems. This mission is accomplished through detection, classification, tracking, reporting and dissemination of data on surface ships, submarines and high interest aircraft. Additional mission areas include gathering long-term oceanographic and geophysical information, support of environmental assessment projects, marine mammal research and counter-narcotics efforts.

1.1 OBJECTIVES

The purpose of this contract is to provide contractor support to Department of the Navy (DoN) Commander, Submarine Force Pacific (COMSUBPAC), Commander, Undersea Surveillance (CUS) or (COMUNDERSEASURV) and other government agencies.

Execution specifically focuses on operations, maintenance, sustainment, and engineering activities, including but not limited to: architecture, design, development, integration, testing, security, and support services. The focus is the deliberate planning, analyzing, organizing, and integrating of current and emerging operational and system capabilities to achieve desired warfighting mission effects, which includes mission analysis, designing or adapting systems and architectures to meet mission outcomes, and analysis and assessments.

1.2 SCOPE

This contract covers the entire spectrum of non-inherently governmental services and solutions (equipment and services) associated with CUS Mission. The Contractor shall provide all personnel, management, supervision, equipment, transportation, tools, supplies, materials, except that which is made available by the Government and specified in order, Government-Furnished Equipment (GFE)/Government Furnished Information (GFI) and Services as defined.

The Contractor systems engineering support to include design, engineering, integration, configuration management, security, testing and operations of new baseline and/or new capability of Commander Undersea Surveillance (CUS), Command, Control, Communications, Computers, Cyber and Intelligence, Surveillance, Reconnaissance (C5ISR) Systems, and associated subsystems located worldwide. This support also includes the implementation and support as an Action Officer for DCNO N2/N6 on matters that pertain to command, control (C2), networks, cyber, intelligence, space, electronic warfare (EW), and maritime domain awareness (MDA), the Information Dominance Corps (IDC), oceanography, and knowledge of the environment. Support personnel shall also support the ISR and undersea capabilities for OPNAV N97.

The Contractor shall provide on-site cyber technical assist support services for C5ISR, and Messaging components and full time support to surveillance facilities in Arlington County, Virginia, Dam Neck,

Virginia, Eugene, Oregon, Dania Beach/Miami, FL, U.S. Naval Station Guantanamo Bay, Cuba, Punta Salinas, P.R., and various CONUS and OCONUS locations. This support includes executive senior level staff work, onsite technical assistance support as well as hardware support of C5ISR and legacy infrastructure, and components at the C5ISR sites.

The Contractor shall provide on-site support services to include C5ISR program management, implementation of current operations, program analyses and implementation, which also includes network modeling and simulation, C5ISR operation case analysis, production control and management, development and portfolio management, technical support services, preventive and casualty maintenance, repairs, installation, requirements generation, budgeting, cost/benefit analysis and cost effective analysis. Other efforts include assisting C5ISR system program management, provide strategic and operational level support, liaise with scientific and technical advisory groups, and technical reviews at program offices located in Washington, D.C., San Diego, and Dam Neck.

The Contractor shall provide all necessary labor, supervision, and management to accomplish the tasks herein.

2.0 SPECIFIC TASKS

2.1 GENERAL

The Contractor must be capable of providing flexible, responsive, and high-quality services and support. The Contractor will conduct travel and reviews that are necessary to ensure the effective and efficient performance of functions identified throughout this Contract which make up this requirement.

The following performance requirements describe the scope of tasks and resources needed to successfully fulfill responsibilities related to this Contract. The Contractor shall provide the necessary timely support to meet emergent requirements as requested by the Contract Officer Representative, Program Manager, Technical Point of Contact, or other properly designated authority. At a minimum, the Contractor will complete all requirements outlined:

2.2 TECHNICAL AND PROGRAM MANAGEMENT, SYSTEMS ENGINEERING, AND DATA ENGINEERING SUPPORT

2.2.1 TECHNICAL AND PROGRAM MANAGEMENT SUPPORT

The Contractor shall have the capability to manage projects applying the Project Management Institute best practices (e.g., Project Management Body of Knowledge, PMBOK). The Contractor shall apply current industry lean and/or agile development best practices to technical efforts that include iterative and incremental project management techniques. Emphasis is on placing capable and supportable systems in the hands of the warfighter when and where needed and at an affordable price.

The Contractor shall facilitate and participate in IPTs, special advisory boards, off sites, working groups, audit teams, etc. The Contractor shall coordinate and monitor meetings, appointments, schedules, and facilities as requested, as well as provide direct support for presentations, conferences, events, and other meetings as requested. The Contractor shall provide good oral and written communications in order to interface with commands and other activities across the Government, DoD, and the Navy. The Contractor shall analyze, evaluate and prepare briefs, reports and correspondence, editing for spelling,

punctuation and grammar, as well as ensuring formats are in compliance with Government, DoD, and Navy procedures.

This support may require significant coordination and interface with various DoD and non-DoD activities located in and out of CONUS.

The contractor shall assess and identify and evaluate the ability of CUS systems to meet existing and emergent mission requirements. This support includes lifecycle maintenance, legacy operational processing systems. Provision of personnel supporting CUS N8 in the development and support of improvements to tactical doctrine and operational procedures.

The contractor shall attend quarterly CUS Program Office meetings in support of development analyses (cost, schedule, and performance), establishing metrics for review and evaluation.

2.2.1.1 Acquisition Management

The Contractor shall support drafting, analyzing, integrating, reviewing, and providing documentation and reports to programmatic leadership in accordance with Government, DOD and Navy regulations. This includes supporting the process of implementing and managing acquisition procurements/ documentation to ensure that documents are properly executed providing proper controls and regulations. The Contractor shall support the development, review and updating of charters, MOAs, MOUs, and organizational charts to enable more effective communications and organizations for the program and stakeholders.

2.2.1.2 Business, Cost Estimating, and Financial Management

The Contractor shall assist the Government in the implementation of fiscal practices and controls. This includes the process of implementing and managing financial control systems, collecting financial data, analyzing financial reports, and making sound financial decisions based on the analyses. The Contractor shall support programming, planning, and budgeting management including budget preparation and justification, funds execution, program planning and analysis, and the presentation of this data in various formats. The Contractor shall analyze, evaluate, and provide recommendations for Total Ownership Cost (TOC) and Life Cycle Cost (LCC). The Contractor shall analyze obligations and expenditures, maintain forecasts, prepare reports on the status/recommendations and availability of funds, justify and prioritize unfunded requirements, and assist with development, review and recommendation of execution year funding efforts.

2.2.1.3 Technical Management

The Contractor shall provide programmatic leadership technical guidance, methodologies in managing, evaluating, providing recommendations, reports, and resolutions. The Contractor shall work with Government stakeholders and technology professionals to properly understand business requirements and develop an industry best practice approach to technology solutions. This includes:

- Evaluating issues and providing recommendations related to system cost, schedule, and performance
- Providing support for requirement generation, allocation, verification, and validation
- Developing and maintain work breakdown structure

- Performing and providing reviews, analyses, studies, documentation, and recommendations for system design including technical expertise in system engineering, software engineering, logistics, test and evaluation and training. Provide recommendations for planning, organizing, and managing critical aspects of the development, production, and/or deployment of capabilities

2.3 SYSTEMS ENGINEERING SUPPORT

The Contractor shall provide systems engineering support for the analysis, design, integration, installation, testing, and life cycle support of new and upgraded systems associated with delivery of capabilities as defined by this Contract. The Contractor shall employ disciplined systems engineering processes in accomplishing Contract tasking, using commercial best practices for systems engineering processes in planning, architecting, requirements development and management, design, technical management and control, technical reviews, technical measurements, integrated risk management, configuration management, data management, interface management, decision analysis, systems management, inspections and maintenance, sources of supply maintenance and repair, and test and evaluation, verification and validation. The Contractor shall provide customer-friendly solutions that provide ease of use for non-technical Government users.

These systems engineering solutions shall follow industry standard engineering processes and may include but not be limited to: Technical assessments of all user requirements, integration of all Government Furnished Equipment (GFE) and Contractor Furnished Equipment (CFE) as proposed, hardware and software information, network applications, system design, initial and recurring training (Commercial Off The Shelf (COTS) or customized), maintenance and support, system interface studies and control documents, network integration and test plans, cost analysis/trade-off studies, engineering change proposals, and engineering support to Government engineers.

The Contractor shall design, develop, test and package systems' changes as well as provide problem resolutions for existing systems according to the project. The Contractor shall maintain the current system baselines and provide change and problem fixes to these baselines as required. The Contractor shall provide to the Government all developed, modified, or converted software, processes, programs, scripts, operating instructions, data models, databases, system files, documentation, test files, and test conditions used to develop each approved systems' change request.

Projects may further refine specific technical approaches and the systems engineering processes according to Government, DoD, or Navy policies and practices. The Contractor shall employ the principles of Open Systems Architecture (OSA), and systems engineering activities used in developing Contractor solutions shall adhere to open architecture designs and employ a modular OSA approach. Projects may require adherence to other governmental standards.

2.3.1 Technology Insertion and Best Practices

The Contractor shall integrate new equipment technologies into existing system architectures as required by applicable Projects. The Contractor shall apply a systems engineering approach to ensure that mission objectives and system criteria requirements are fulfilled. Emphasis shall be on the demonstration of clear and definable improvements in the performance, logistics supportability, reliability and maintainability of the item. All efforts shall employ the latest technology in consonance with economic considerations.

The Government is interested in remaining current and knowledgeable in the latest industry trends that affect the technology provided to their customers. When requested, the Contractor shall provide white papers and briefings to agency management that includes the following information:

- The latest industry trends in the functional areas supported under the applicable Project. The Contractor shall provide suggestions for change to the operation and configuration of the infrastructure environment, as appropriate and as required, that will ensure that the agency remains current, efficient, and effective and so that the users continue to receive a high level of quality support. The white paper should include a cost benefit analysis of the suggested change.
- Research and identification of system requirements and recommendations of technology solutions to project and technical leadership
- Research and investigation of new technologies and their possible use by systems covered under applicable Projects. Services shall include ongoing evaluation of current technology, platforms, and operations to seek improvement and optimal business processes. The Contractor shall identify and recommend best practices and best technology for the Government needs and responsibilities.

2.3.2 Technical Development Reviews

The Contractor shall conduct formal and informal technical reviews as well as periodic technical development reviews for major capability upgrades. The purpose of these reviews is to observe that the design and other documentation is complete, complies with the established design and testing approach, is technically sound and will satisfy the functional requirements as defined in the approved functional design specification documents.

Technical Review Objectives:

- Analyze and design hardware, based off the NC3 circuit modernization architecture, for data mining, warehousing and processing systems used on C5ISR systems, and autonomous and non-autonomous systems.
- Analyze and design analog and digital test interfaces for signal analysis, signal conditioning, signal processing, information processing, display processing, and make recommendations for concepts or enhancements for C5ISR maritime and littoral area surveillance, and autonomous and non-autonomous systems. Perform research in automated search methodology for target detection and tracking. Research latest technical information related to C5ISR systems, and autonomous and non-autonomous systems and subsystems. Predict the performance of current surveillance systems and future surveillance systems by selecting appropriate parameters for existing models and analyzing the results. Reduce and process data by using contractor and government facility.
- Analyze and design fiber optic cable and electronic systems with fiber optic interfaces, including telemetry and networked systems and autonomous and non-autonomous systems. Measure and analyze optical cable parameters of fiber-optic cable. The contractor shall provide technical support services for the operation, maintenance and repair of signal processing, acoustic data collection, and communications equipment and backup support systems.
- Analyze and design cable handling systems for C5ISR systems.
- Ensure operational, functional, performance, information assurance, cost, schedule requirements

and objectives, designs, implementations, technical performance measurements, and technical plans are being tracked, are on schedule, and are achievable within existing programmatic constraints.

- Assess the system requirements and allocations to ensure that requirements are unambiguous, traceable to top-level requirements.
- Demonstrate that the relationships, interactions, interdependencies, and interfaces between required items and externally interfacing items, system functions, subsystems, and system elements (including operators and maintainers), as appropriate, have been addressed.
- The contractor shall prepare engineering drawings, design documents, parts list, and technical reports for assigned surveillance systems.

2.3.3 System Supportability and Readiness

The Contractor shall participate in the systems engineering process to impact the design from inception throughout the life cycle, facilitating supportability to maximize the availability, effectiveness, and capability of the system at the lowest life cycle cost. Readiness and support resource requirements and design parameters include the following:

- Human factors to improve warfighter capability
- User/machine/software/interface/usability
- System safety
- Reliability, availability, maintainability (RAM)
- Survivability and vulnerability
- Standardization and interoperability
- Analyze and design signal-processing algorithms, signal characteristics, and signal extraction techniques. Analyze the propagation of acoustic and non-acoustic energy through the ocean and air media.
- Identify and evaluate processing and display technologies internal and external to the CUS community in active and passive signal processing, automation, situational awareness, contact management, localization and tracking, reporting, communications, satellite and terrestrial bandwidth management, operator-machine interface (OMI), training and sensor performance prediction that would allow CUS processing systems to more effectively meet current and future undersea warfare processing requirements.

2.4 CONFIGURATION MANAGEMENT (CM) SUPPORT

The Contractor shall identify, document, and verify the functional, performance, and physical characteristics of systems and associated interface systems, to control changes and non-conformance, and to track actual configurations of systems and platforms. Using MIL-HDBK-61A as guidance, the Contractor shall provide support that includes all activities related to CM planning, baseline management, configuration identification, configuration audits, formal reviews, engineering changes, and configuration management records and reports; and the use of automated tools to perform these functions. CM support requirements including the following:

- The contractor shall maintain a report and record system, and provide current status of all electronic equipment, which includes documenting revisions to instructions and operating procedures.

- The contractor shall maintain configuration control in government database program, Microsoft Sharepoint, and configuration management of equipment drawings to ensure accuracy when system, equipment or infrastructure changes are made.
- The contractor shall create and maintain CUS data models to collect maintenance, communications, and systems operations performance and reliability data.
- The contractor shall create and maintain CUS data models to collect Fixed Systems watch team key performance metrics.

2.5 DATA ENGINEERING SUPPORT

The Contractor shall provide data engineering support for the analysis, design, integration, installation, testing, and life cycle support of new and upgraded systems associated with delivery of capabilities as defined by this Contract. Data engineering covers the architecture, design, development, integration, and testing of systems that access, collect, ingest, clean, analyze, store, visualize, and share data. This includes software development and system administration support to Surveillance specific technologies. The Contractor shall employ commercial best practices as required by applicable. The Contractor shall provide customer-friendly solutions that provide ease of use for non-technical Government users.

Projects may further refine specific technical approaches and the data engineering processes according to Government, DoD, or Navy policies and practices. The Contractor shall employ the principles of OSA, and data engineering activities used in developing Contractor solutions shall adhere to open architecture designs and employ a modular OSA approach. Projects may require adherence to other governmental standards.

The contractor shall provide readiness, reliability, and other specified data collection and analysis in support of organization requests. Create appropriate metric models to monitor and form trend data analysis. Prepare visual presentations of quantitative information.

2.6 GENERAL ENGINEERING SUPPORT

2.6.1 STUDY AND ANALYSIS

The Contractor shall perform studies and analyses as required by applicable Projects. Such studies/analyses may include engineering, scientific, financial, operational, etc. considerations for acquisition efforts. The Contractor shall perform non-recurring engineering studies and analyses to evaluate the viability of potential solutions to solve various technical problems or meet system requirements. These studies and analysis include the assessment of system and subsystem requirements; development, analysis and evaluation of concepts, technologies, systems and subsystems; and development and examination of operational concepts and tactics. Results shall be documented and submitted as required by applicable Projects. Studies and analysis requirements including the following:

- Analyze test results and generate analysis reports for various supporting autonomous and non-autonomous systems and subsystems.
- Analyze data on threat operating patterns. Create and maintain a presence model in support of requirements and scheduling.

2.6.2 INSTALLATION AND INTEGRATION

The Contractor shall install and integrate hardware and software as required by applicable Projects to include Command and Control Platforms and sensors into platforms. Installation may involve fabrication of mounts, brackets, and/or installation kits to include cabling, connections, and interconnecting devices. This includes the development of installation and integration plans, drawings, technical change documentation and notices and procedures in support of these efforts.

When required, the Contractor shall assist the Government in identifying all equipment and utilities required for installation at the installation site, including Government Furnished Equipment/Material. The Government, with Contractor assistance, shall ensure that the required equipment, utilities, and resources are available at the installation site. The Contractor shall identify, plan, resource, and acquire Packaging, Handling, Storage and Transportation (PHS&T) requirements to maximize availability and usability of materiel and equipment to include support items whenever they are needed for training or other aspects of the mission. Installation and Integration requirements including the following:

- Integrate and assemble, analog and digital hardware test interfaces, designed for signal analysis, signal conditioning, signal processing, information processing and display processing for C5ISR maritime and littoral area surveillance, and autonomous and non-autonomous systems and subsystems.
- Integrate fiber optic cable and electronic systems with fiber optic interfaces including telemetry and networked systems.
- Integrate and assemble cable handling systems, for C5ISR systems. Support requires expertise in the operation of electric and hydraulic winch systems, heavy duty equipment, and maritime equipment in direct support of installation operations.
- Installation of critical utilities and infrastructure by means of Horizontal Directional Drilling (HDD).
- Integrate software used in the operation or test of C5ISR autonomous and non-autonomous systems and subsystems.
- Integrate electronic, acoustic, optical, or mechanical interfaces, required by C5ISR non-autonomous systems and subsystems.

2.6.3 TRAINING

The Contractor shall plan, resource, implement, and conduct a cohesive integrated strategy to train military and civilian personnel to maximize the effectiveness of the doctrine, manpower and personnel, to fight, operate, and maintain systems, software, and equipment throughout the life cycle.

The Contractor shall support the development of training policy, processes, procedures, techniques, training devices, and equipment used to train civilian and military personnel to acquire, operate and support a system. This includes individual and crew training, new equipment training, initial, formal, and on-the-job training, as well as training during system development to support the system test and evaluation.

The contractor shall develop technical manuals, step-by-step operator/maintenance manuals, concept of operations manuals, operation guidelines, and operating procedures.

The contractor shall conduct training courses (one per site, approximately 20 sites) for C5ISR

autonomous and non-autonomous systems and subsystems supporting DoD surveillance operations.

2.6.4 FACILITIES EMPLACEMENT, RENOVATIONS, AND/OR IMPROVEMENTS

The contractor shall design and/or perform facility emplacement, renovations, and/or improvements necessary to achieve required functionality and systems integration. Such facility modifications may be accomplished CONUS and OCONUS and can include, but are not limited to, environmental, architectural, engineering, management, and installation as it relates to the technical requirements.

2.6.5 TEST AND EVALUATION

The Contractor shall define and develop test programs, plans, and procedures, conduct testing, and evaluate and document results. Such testing may include:

- 2.6.5.1 Hardware and software component testing
- 2.6.5.2 Subsystem and system level development testing
- 2.6.5.3 System compatibility testing
- 2.6.5.4 Acceptance testing
- 2.6.5.5 Functional testing
- 2.6.5.6 Integration testing
- 2.6.5.7 Full qualification testing
- 2.6.5.8 Field-testing and evaluation
- 2.6.5.9 Environmental tests and stress screening
- 2.6.5.10 Electromagnetic interference testing, electromagnetic compatibility testing and TEMPEST

The Contractor shall conduct testing in total or shall support Government test personnel as required. The Contractor shall ensure that all hardware, software, test equipment, instrumentation, supplies, facilities, and personnel are available and in place to conduct or support each scheduled test.

The Contractor shall review and evaluate Test Evaluation Master Plans, test plans, test procedures and test results as required.

The contractor shall perform and/or apply engineering, scientific analytical disciplines and the development of all necessary test documentation, plans, change requests, specifications and reports to ensure that developed platforms, C5ISR and IT systems, and war-fighting capabilities have been properly tested and that joint interoperability requirements have been fully met at all levels of its life cycle; including the support of measurement facilities, ranges and instrumentation used for testing, evaluating, experimenting, and exercising platforms and systems.

2.7 CYBER SECURITY SUPPORT

The Contractor shall review existing security policies and procedures, whether formal or informal. The Contractor shall work closely with the Information Assurance Manager (IAM) and staff to develop formal policies and procedures to facilitate the protection of U.S. Government sensitive unclassified and classified information and the security of the various information systems and networks. The Contractor shall review existing policies, procedures and guidelines and shall draft appropriate policy documents

for implementation across the enterprise as directed by the IAM.

The Contractor shall assist appropriate government personnel in determining information assurance (IA) requirements, aid in the development of policies and procedures for implementation and provide support in implementing these mechanisms and processes to ensure that the policies can be enforced. This includes Information Assurance Vulnerability Alert (IAVA) tracking, compliance with Defense Information Systems Agency (DISA) Application Security Development Security Technical Implementation Guides (STIG), System Administrator certification, and all other activities that contribute to the successful implementation of the full range of IA policies, procedures, and guidelines.

The Contractor shall ensure that all system or application deliverables meet the requirements of DoD or applicable Information Assurance (IA) policies. The Contractor shall adapt to emerging DoD, DoD component, and OGA policies (e.g. NIST) as they are enacted. This support includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. The Contractor shall ensure security requirements are addressed during engineering design and development.

The Contractor shall support Commissioning and Acceptance of systems in accordance with governing policies. The Contractor's IA system owner support includes services such as conducting system assessments, identifying/implementing modifications to bring systems into compliance, recommending security risk mitigation solutions, preparing accreditation packages, and supporting generation of acquisition milestone documentation. The Contractor shall conduct security scans, document vulnerabilities, correct vulnerabilities, and document the resolution or mitigation of vulnerabilities.

The contractor shall provide monthly scans of all systems/networks, apply patches and Information Assurance Vulnerability Assessments (IAVAs) to mitigate monthly scan findings, and provide reporting post scan actions to the Information Assurance Manager (IAM).

The contractor shall provide assistance in maintaining command Websites.

The contractor shall conduct tests of DISA Field Engineering Notice (FEN) procedures, Vendor IAVAM's, and patches within thirty (30) days of release. The contractor shall document minor changes to baselines and capabilities.

The contractor shall provide all elements of CYBER Security & Defense, RMF processing and approval, to include:

- a. Assess network infrastructure and bring the system up to all required IA standards.
- b. Complete thorough RMF/C&A process and complete the certification package for submission to the C&A officials.
- c. Create and make corrections to C&A packages and track through the IA process.

2.8 IN-SERVICE ENGINEERING AND SERVICE DESK SUPPORT

The Contractor shall support 24/7/365 in-service and service desk management. This includes providing technical assistance, warranty support, and system maintenance. The Contractor shall provide methods for responding to customer requests and reporting, resolving, and closing deficiencies. The Contractor shall monitor in-service and service desk reports, provide performance improvement recommendations, identify environmental changes and changes in Government equipment or regulations and make the recommended performance improvement, environmental, or equipment changes as requested by the Government.

The contractor shall perform and/or apply engineering, scientific analytical disciplines to all aspects of In-Service Engineering Activities (ISEA) tasking of Enterprise Life cycle Sustainment Services to include Technical Sustainment Support, including Distance Support, On-Site Support, and Proactive Sustainment, Modernization Support of Systems Operational Verification Test (SOVT) and Software Loads, and Life cycle Sustainment Engineering and testing in accordance with the COMUSFLTFORCOMINST 4790.3, Joint Fleet Maintenance Manual (JFMM) and other direction. This includes Fleet Support Services Center support of Casualty Reports (CASREPs) and urgent requests for Technical Assistance, Modernization support of SOVT and Software Loads for system installations, and system expertise in Life cycle sustainment activities.

In support of the 24/7/365 in-service and service desk management the Contractor shall:

- Provide technical assistance of deployed systems will include phone, email, and on-site support to restore C5ISR systems customers back to operational condition. Estimated forty (40) phone calls and forty (40) emails for technical assistance responses are anticipated per month for all systems, components and associated subsystems referred in paragraph 1.0. Emails and phone calls shall be answered within one (1) business day.
- Provide technical assistance (Tier 3) and hardware failure repair and restoration for C5ISR and Legacy Messaging components located at DSP sites referred in paragraph 1.0. The contractor shall provide Tier 4 support including phone and email interaction, with travel to sites to maintain operations, correct Casualty Reports (CASREPs) at Naval Ocean Processing Facilities (NOPFs), operational fleet activities listed in Applicable Document 2.10, and Messaging Service Providers.
- Respond via phone or email to all DSP CASREPs within 30 minutes of notification and IAW Applicable Documents 2.13 through 2.15. In response to trouble calls and CASREP situation requiring onsite support, the contractor shall provide onsite support to restore systems to operational status. The contractor shall conduct root cause analysis and provide recommendation for equipment modifications, installations and repairs. The contractor shall report system casualties or degradations and assist with systems restoration.
- Provide general maintenance and corrective actions on C5ISR and Naval Messaging and Department of Defense Messaging systems located at various worldwide facilities. Maintenance shall include day to day monitoring of equipment condition, performance, diagnostic testing, corrective actions, and restoration of the system components related to system hardware and software.
- Provide a N97 Cable Subject Matter Expert (SME) who shall provide both remote and on scene assessment of ongoing Fleet efforts for DoD components and other government agencies as required. Interact with Fleet Staffs and NAVY components in the formulation of schedule and program execution.
- Provide direct onsite (for all CUS shore sites) systems management of various networks and systems and provide systems administration (including remote) of several servers and workstations and hundreds of associated networks, cryptographic, and peripheral devices.
- Support all CUS systems by developing progress reports, identifying risk/issues, offer solutions and providing resolution status.
- Create and maintain inventories/classified control of all CUS assets.
- Perform all required preventive and corrective calibration, alignment and testing procedures for the installed support equipment. The contractor shall provide support to achieve maximum operational readiness of all electronic equipment/systems, to include: back-up power; Heating

Ventilation and Air Conditioning (HVAC); and security (Intrusion Detection, Access Control, Surveillance) by performing operational tests and maintenance procedures. This includes conducting surveys, root cause analysis and investigation to determine system design problems, preservation work, assessments, design and restoration of all equipment by performing operational tests and maintenance procedures.

3.0 CONTRACT ADMINISTRATION

Contract administration is required for all contracts; it provides the government a means for contract management and monitoring. Regardless of the level of support, the ultimate objective of the contractor is ensuring the government's requirements are met, delivered on schedule, and performed within budget.

3.1 CONTRACT LIAISON

The contractor shall assign a technical single point of contact, also known as the Program Manager (PM) who shall work closely with the government Contracting Officer and Contracting Officer's Representative (COR), as applicable. The contractor PM, located in the contractor's facility, shall ultimately be responsible for ensuring that the contractor's performance meets all government contracting requirements within cost and schedule. PM shall have the requisite authority for full control over all company resources necessary for contract performance. The PM shall have authority to approve Project proposals or modifications in emergent situations. The PM shall ultimately be responsible for the following: personnel management; management of government material and assets; and personnel and facility security. In support of open communication, the contractor shall initiate, unless otherwise directed at the Project level, periodic meetings with the COR.

3.2 CONTRACT MONITORING AND MAINTENANCE

The contractor shall have processes established in order to provide all necessary resources and documentation during various times throughout the day in order to facilitate a timely award or modification. To address urgent requirements, the contractor shall have processes established during business and non-business hours/days in order to provide all necessary documentation and resources to facilitate a timely award or modification.

3.2.1 CONTRACT ADMINISTRATION DOCUMENTATION

Various types of contract administration documents are required throughout the life of the contract. At a minimum, the contractor shall provide the following documentation, unless otherwise specified:

3.2.1.1 Management Plan

The contractor shall develop and submit a Management Plan for detailing its technical and management approach for accomplishing this contract objectives. The contractor's successful proposal will satisfy the requirements for the first submission of the management plan.

A revised management plan will be required on as-needed basis in response to changes in scope, required resources, and/or order ceiling revisions. The contractor shall submit revised management plan to the Contracting Officer within ten (10) business days after receiving written notification from the Contracting Officer that a management plan revision is required or after a contract modification is issued necessitating a revision to scope, resources, and/or ceiling values. The revised management plan shall provide the contractor's detailed approach to accomplishing the requirements of the contract changes and

will identify the contractor's overall estimate for completing the task.

3.2.1.2 Contract Status Reporting

The contractor shall develop a Contract Status Reports and submit it monthly, weekly, and/or as cited in the requirements of each order. The prime shall be responsible for collecting, integrating, and reporting all subcontractor reports. The status report includes the following variations of reports:

- (a) Monthly Status Report (MSR) – the contractor shall develop and submit a BPA-status report ~~monthly at least 30 days after BPA award on the 20th of each month for those months the BPA is active.~~ The contractor shall report on various order functions: performance, schedule, financial, business relations, and staffing plan/key personnel. This CDRL includes a Staffing Plan, Personnel Listing, and Government Furnished Property (GFP) Template necessary for additional data collection as applicable.
- (b) ~~Weekly Status Report – the contractor shall develop and submit a weekly status report which is e-mailed to the COR no later than close of business (COB) every Friday. The first report is required on the first Friday following the first full week after the contract award date. The contractor shall ensure the initial report includes a projected Plan of Action and Milestones (POA&M). At a minimum unless otherwise noted, the contractor shall include in the weekly report the following items and data:-~~
- ~~1. Percentage of work completed~~
 - ~~2. Percentage of funds expended~~
 - ~~3. Updates to the POA&M and narratives to explain any variances~~
 - ~~4. If applicable, notification when obligated costs have exceeded 75% of the amount authorized~~
- (c) Data Calls – the contractor shall develop and submit a data call report which is e-mailed to the COR within forty-eight working hours of the request, unless otherwise specified. The contractor shall ensure all information provided is the most current. Cost and funding data will reflect real-time balances. Report will account for all planned, obligated, and expended charges and hours. At a minimum unless otherwise noted, the contractor shall include in the data call the following items and data:
1. Percentage of work completed
 2. Percentage of funds expended
 3. Updates to the POA&M and narratives to explain any variances
 4. List of personnel (by location, security clearance, quantity)
 5. Most current GFP and/or CAP listing

The contractor shall develop a order closeout report and submit it no later than 15 days before the order's completion date. The Prime shall be responsible for collecting, integrating, and reporting all subcontracting information.

3.2.1.3 MATERIALS Limitation Notification

Contractors shall monitor MATERIAL costs as part of the monthly contract status reports. For this monitoring purpose, MATERIALSs include incidental material, travel, and other non-labor costs (excluding subcontracting and consultant labor cost) required in performance of the service. For any given period of performance, if the cumulative total cost of MATERIALSs exceeds the awarded total cost of MATERIALSs (regardless of any modifications to the awarded amount) by 10%, the contractor shall send notice and rationale for exceeding cost to the COR who will then send a memorandum signed by the PM (or equivalent) to the Contracting Officer documenting the reasons justifying the increase of MATERIALS.

4.0 QUALITY

4.1 QUALITY SYSTEM

Upon contract award, the prime contractor shall have and maintain a quality assurance process that meets contract requirements and program objectives while ensuring customer satisfaction and defect-free products/process. Due to the nature, size and complexity of this requirement CUS is mandating that the prime contractor carry ISO 9001:2015 certification. Offerors need to be ISO 9001:2015 certified at time of proposal submission. The contractor shall have a sufficiently documented quality system which contains procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system based on a contractor's internal auditing system. Thirty (30) days after contract award, the contractor shall be able to provide to the government a copy of its Quality Assurance Plan (QAP) and any other quality related documents as applicable to the contract. The contractor shall make the quality system available to the government for review at both a program and worksite services level during predetermined visits. Existing quality documents that meet the requirements of this contract may continue to be used. If any quality documentation is disapproved or requires revisions, the contractor shall correct the problem(s) and submit revised documentation NLT 2 weeks after initial disapproval notification. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan and development of quality related documents as needed. At a minimum, the contractor shall ensure their quality system meets the following key criteria:

- Establish documented, capable, and repeatable processes
- Track issues and associated changes needed
- Monitor and control critical product and process variations
- Establish mechanisms for feedback of field product performance
- Implement and effective root-cause analysis and corrective action system
- Establish methods and procedures for continuous process improvement

4.2 QUALITY MANAGEMENT PROCESS COMPLIANCE

4.2.1 GENERAL

The contractor shall have processes in place that coincide with the government's quality management processes. The contractor shall use best industry practices including, when applicable, ISO/IEC 15288 for System life cycle processes and ISO/IEC 12207 for Software life cycle processes. As applicable, the contractor shall also support and/or participate in event-driven milestones and reviews as stated in the Defense Acquisition University's (DAU's) DoD Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System Chart which is incorporates multiple DoD directives and instructions – specifically DoDD 5000.01 and DoDI 5000.02.

4.2.2 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified by the respective WBS, POA&M, or quality system, and the

contractor shall deliver related quality plan/procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related services, documents, and material in a category when noncompliance is established.

4.2.3 QUALITY CONTROL

The contractor shall have a sufficiently documented quality system which contains procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system based on a contractor's internal auditing system. Thirty (30) days after contract award, the contractor shall be able to provide to the government a copy of its Quality Assurance Plan (QAP) and any other quality related documents as applicable to the contract. The contractor shall make the quality system available to the government for review at both a program and worksite services level during predetermined visits. Existing quality documents that meet the requirements of this contract may continue to be used. If any quality documentation is disapproved or requires revisions, the contractor shall correct the problem(s) and submit revised documentation NLT 2 weeks after initial disapproval notification. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan and development of quality related documents as needed. At a minimum, the contractor shall ensure their quality system meets the following key criteria:

- Establish documented, capable, and repeatable processes
- Track issues and associated changes needed
- Monitor and control critical product and process variations
- Establish mechanisms for feedback of field product performance
- Implement and effective root-cause analysis and corrective action system
- Establish methods and procedures for continuous process improvement

4.2.4 QUALITY MANAGEMENT DOCUMENTATION

In support of the contract's Quality Assurance Surveillance Plan (QASP) and Contractor Performance Assessment Reporting System (CPARS), the contractor shall provide the following documents: Cost and Schedule Milestone Plan submitted 10 working days after order award.

4.2.5 INSPECTION AND ACCEPTANCE CRITERIA

Inspection and acceptance criteria for all deliverables shall adhere to the methods standards outlined in the QASP. The contractor shall deliver a draft QASP within 15 working days of contract award, with a finalized QASP (to be negotiated with the Government) delivered no later than 30 working days after contract award.

4.3 INFORMATION SYSTEM

4.3.1 ELECTRONIC COMMUNICATION

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the government. The contractor shall be capable of Public Key Infrastructure client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on contract shall be accessible by e-mail through individual accounts during all working hours.

4.3.2 INFORMATION SECURITY

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

4.3.2.1 Safeguards

The contractor shall protect government information and shall provide compliance documentation validating they are meeting this requirement in accordance with DFARS clause. The contractor and all utilized subcontractors shall abide by the following safeguards:

- (a) Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.
- (b) Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.
- (c) Sanitize media (e.g., overwrite) before external release or disposal.
- (d) Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. NOTE: Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DOD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage." The contractor shall ensure all solutions meet FIPS 140-2 compliance requirements.
- (e) Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.
- (f) Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption.

(g) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

(h) Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

(i) Provide protection against computer network intrusions and data exfiltration, minimally including the following:

1. Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.
2. Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.
3. Prompt application of security-relevant software patches, service packs, and hot fixes.

(j) As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).

(k) Report loss or unauthorized disclosure of information in accordance with contract or agreement requirements and mechanisms.

4.3.2.2 Compliance

Pursuant to DoDM 5200.01, the contractor shall include in their quality processes procedures that are compliant with information security requirements.

4.4 SECURITY

4.4.1 ORGANIZATION

At time of award, all key personnel, as listed below, require an active security clearance. In accordance with clause 5252.204-9200 and the DoD Contract Security Classification Specification, DD Form 254, classified work is performed under this contract. The contractor shall have at the time of contract award and prior to commencement of classified work, a TOP SECRET facility clearance (FCL). The initial DD-254 issued is TOP SECRET with Sensitive Compartment Information (SCI) and Special Access Program (SAP) access.

4.4.2 PERSONNEL

4.4.2.1 Key Personnel Descriptions

Operations Program Manager (PgM). A PgM with strategic program leadership experience backed up by hands-on operational leadership experience in all objective areas will provide effective governance and leadership. The Government should consider the following experience and qualifications for a PgM key position:

- Shielding Effectiveness Testing Certified with a minimum of 10 years of operational testing experience
- Construction of Electromagnetically Shield Enclosures Certified
- Clearance: Existing TS/SCI
- Subject Matter Expert (SME) level experience ~~25 years~~ managing and supervising employees in various LCATS and skills
- SME level experience ~~20 years~~ managing multi-disciplined and geographically separated delivery teams
- SME level experience ~~40 years~~ managing projects whose scope included architecture and construction of complex mission-critical facility green field and renovations, environmental assessments, and infrastructure modernization projects to include C5ISR
- SME level experience, minimum of 10~~5~~ years managing OCONUS design/build projects
- Experience translating TO requirements into project plans and milestones
- Experience managing large teams across multiple geographies
- Excellent oral and written communication skills at the senior DoD executive audiences

Engineering Program Manager (PgM). A PgM with strategic program leadership experience backed up by hands-on operational leadership experience in all objective areas will provide effective governance and leadership. The Government should consider the following experience and qualifications for a PgM key position:

- Master's Degree in Systems Engineering
- Project Management Professional (PMP) Certification
- Design Build Institute of America (DBIA) Certification
- Clearance: Existing TS/SCI
- ~~25 years~~SME level experience managing and supervising employees in various LCATS and skills
- ~~20 years~~SME level experience managing multi-disciplined and geographically separated delivery teams
- ~~45 years~~SME level experience managing projects whose scope included architecture and construction of complex mission-critical facility green field and renovations, environmental assessments, and infrastructure modernization projects to include C5ISR
- SME level experience, minimum of 10~~5~~ years managing OCONUS design/build projects
- Experience translating TO requirements into project plans and milestones
- Experience managing large teams across multiple geographies
- Excellent oral and written communication skills at the senior DoD executive audiences

Project Manager (PM). A PM with strategic project management experience backed up by hands-on operational management experience in all objective areas will provide effective governance and leadership. The Government should consider the following experience and qualifications for a PM key position:

- Bachelor's Degree

- PMP Certification
- Clearance: Existing TS/SCI
- ~~10 years~~ SME level experience managing and supervising employees in various LCATS and skills
- ~~10 years~~ SME level experience managing multi-disciplined and geographically separated delivery teams
- ~~10 years~~ SME level experience management experience in project planning, requirements development, project management of complex mission-critical facility renovations, environmental upgrades, and infrastructure modernization projects
- SME level experience, minimum of 10 years managing OCONUS design/build projects
- Experience translating TO requirements into project plans and milestones
- Experience managing large teams across multiple geographies
- Excellent oral and written communication skills at the senior DoD executive audiences.

Operations Manager. An Operations Manager with deep IUSS technical mission expertise, proven operational qualifications backed up by hands-on, operational leadership experience in all objective areas will provide effective leadership and governance. The Government should consider the following recommended experience and qualifications for Operations Manager key position:

- Bachelor's Degree
- Clearance: Existing TS/SCI
- SME level of experience ~~20 years~~ leading ~~CUS~~ IUSS/ASW mission operations across multiple operational theaters and varying mission sets
- ~~10 years~~ SME level of experience leading resource utilization, policies, and requirements for ~~CUS~~ IUSS/ASW operations
- Expertise in contract technical lead delivery of ~~CUS~~ IUSS mission operations
- Experience leading large teams across multiple geographies
- Excellent oral and written communications skills at the DoD senior audiences
- Experience in architecture and construction of complex mission-critical facility renovations, environmental upgrades, and infrastructure modernization projects to include C5ISR

Engineering and Technical Lead. An Engineering and Technical Lead with proven capabilities in systems analysis and trades, coordinating engineering activities, engineering baseline management, interface management, requirements/V&V management, subcontractor technical oversight, preparing/presenting SE material at all major reviews and PMRs, and interfacing with the customer and stakeholders on all technical issues. The Government should consider the following recommended experience and qualifications for Engineering and Technical Lead key positions:

- Master's degree in electrical engineering
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Privacy Technologist (CIPT)
- Clearance: Existing TS/SCI

- ~~20 years'~~SME level of experience in networking and system design, implementation, and lifecycle maintenance
- ~~20 years'~~SME level of experience working with windows servers
- ~~20 years'~~SME level of experience design and building IT networks with various manufacturers
- Experience leading cross-discipline teams
- Experience in advanced analytical problem solving, and negotiation and organizational skills with demonstrated ability to multi-task, organize, prioritize, and meet deadlines

Engineering and Technical Lead. An Engineering and Technical Lead with proven capabilities in systems analysis and trades, coordinating engineering activities, engineering baseline management, interface management, requirements/V&V management, subcontractor technical oversight, preparing/presenting SE material at all major reviews and PMRs, and interfacing with the customer and stakeholders on all technical issues. The Government should consider the following recommended experience and qualifications for Engineering and Technical Lead key positions:

- Bachelor's degree in Electrical Engineering
- Clearance: Existing TS/SCI
- ~~40 years'~~SME level of experience supporting IUSSCUS, EKMS, and Fixed Facility Surveillance systems
- ~~40 years'~~SME level of experience working with diverse teams of engineers across a wide geographic area
- ~~40 years'~~SME level of experience designing electrical systems, grounding systems, and DC power systems
- Experience in advanced analytical problem solving, and negotiation and organizational skills with demonstrated ability to multi-task, organize, prioritize, and meet deadlines

Network Engineer. A Network Engineer with demonstrable capabilities in the research, development, implementation, testing, and review of network infrastructure to include, routing, switching, VoIP, firewalls, IDS, and crypto devices. This role will provide direct engineering support and supervise a team of lower level engineers to accomplish mission objectives. The Government should consider the following recommended experience and qualifications for Network Engineer key position:

- Bachelor's degree in Information Technology
- Cisco Certified Network Professional (CCNP)
- Public ATM Switch Product Specialist Certified
- Security + Certified
- Clearance: Existing TS/SCI
- ~~45 years'~~SME level of experience in the design of routing and switching networks
- ~~45 years'~~SME level of experience in the installation and testing of routing and switching networks
- SME level of experience, minimum of 10~~5~~ years' experience hardening networks and systems per 8500.1 and 8500.2 policies and procedures

Undersea Cable System Subject Matter Expert (SME). An Undersea Cable System SME

with demonstrable capabilities in the installation, operation, maintenance, and repair of undersea cable systems, outside plant and associated transmission equipment. The Undersea Cable System SME shall be responsible for planning, organizing, and implementing projects in support of the design, development, and testing of undersea cable systems architecture, components, or products and interfacing with the customer and stakeholders on all technical issues. The Government should consider the following recommended experience and qualifications for Undersea Cable System SME key position:

- SME level of experience, minimum of 15~~30~~ years' experience in the installation and repair of fiber optic and analog undersea cables.
- SME level of experience, minimum of 15~~30~~ years' experience in the utilizing specific test equipment (COTDR, OTDR, etc.) to test and monitor Submarine Cable systems.
- SME level of experience, minimum of 10 years' experience in multiple aspects of Submarine Cable installation engineering, installation and repair aboard domestic and foreign platforms. Specifically, experience in functioning as an Engineer in Charge, Power Safety Officer, and Transmission Engineer.
- SME level of experience, minimum of 10 years' experience using route survey data to create installation plans and methods of procedure for installation and repair evolutions
- Clearance: Existing TS/SCI

RF Engineer. A RF Engineer with demonstrable capabilities in the design of RF systems to include electromagnetic analysis and testing of electromagnetic interference capabilities. The RF Engineer shall be responsible for planning, organizing, and implementing projects in support of the design, development, and testing of RF systems architecture, components, circuits, or products. The Government should consider the following recommended experience and qualifications for RF Engineer key position:

- Clearance: Existing TS/SCI
- ~~15 years'~~ SME level of experience in the design of RF systems
- SME level of ~~15 years'~~ experience in the implementation of RF systems
- SME level of ~~15 years'~~ experience in the testing of RF systems
- SME level of ~~15 years'~~ operational experience in Electromagnetic Effects
- SME level of ~~15 years'~~ experience with DoD survivability assessments and mission assurance guidance
- SME level of ~~15 years'~~ experience in addressing EM protection as it applies across a broad RF spectrum

4.4.2.2 SECURITY OFFICER

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring clearance and/or access to government facility/installation and/or access to information technology systems under this contract. The FSO is key management personnel who is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher than the FCL required on this contract. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on contract. Responsibilities include entering and updating the personnel security related and mandatory training information within the Staffing Plan document, which is an attachment to the contract status report (CSR). FSO shall also update and track data in the Cyber Security Workforce (CSWF).

4.4.2.3 CONTRACT MANAGEMENT OF THIS CONTRACT, PROGRAM MANAGER

The Contractor shall designate a single Program Manager to oversee the contractor's performance under this contract. The Contractor's designated Program Manager shall serve as the single point of contact for addressing contractor performance issues, quality issues, and overall Contractor performance. This may include coordination with the contract office and the COR to resolve any issues that may arise, trends relating to this contract, proposed changes or modifications to this contract. The Program Manager will be considered Key Personnel for this Contract.

4.4.2.4 KEY PERSONNEL

The Contractor shall meet the minimum personnel qualifications for each of the Key Personnel identified in Section 4.4.2.1, the education, skills, and abilities are applicable specifically to this Contract:

The contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M – National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30, DoD 8570.01-M, and the Privacy Act of 1974. Prior to any labor hours being charged on contract, the contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the contract/order, and if applicable, are certified/credentialed for the Cybersecurity Workforce (CSWF). A favorable background determination is determined by either a National Agency Check with Inquiries (NACI), National Agency Check with Law and Credit (NACLC), or Single Scope Background Investigation (SSBI) and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to government installations/facilities, government IT systems and IT resources. *Cost to meet these security requirements is not directly chargeable to BPA.*

4.4.2.5 PERSONNEL CLEARANCE

Some personnel associated with this contract shall possess a TOP SECRET with SSBI personnel security clearance (PCL). At the Government's request, on a case-by case basis, Top Secret (TS) clearances that consist of a Single Scope Background Investigation (SSBI) are eligible for access to Sensitive Compartmented Information (SCI). These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data as applicable. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the Department of Defense Consolidated Adjudications Facility (DoD CAF) and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, DoD Instruction for Cybersecurity. Contractor personnel shall handle and safeguard any Controlled Unclassified Information (CUI) and/or classified information in accordance with appropriate Department of Defense and Navy security regulations.

4.4.2.6 ACCESS CONTROL OF CONTRACTOR PERSONNEL

4.4.2.6.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the government facility/installation.

- The majority of government facilities require contractor personnel to have an approved visit request on file at the facility/installation security office prior to access. The contractor shall initiate and submit a request for visit authorization to the COR in accordance with DoD 5220.22-M (NISPOM) not later than one (1) week prior to visit – timeframes may vary at each facility/installation.
- Depending on the facility/installation regulations, contractor personnel shall present a proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement.
- All contractor persons engaged in work while on Government property shall be subject to inspection of their vehicles at any time by the Government and shall report any known or suspected security violations to the Security Department at that location.

4.4.2.6.2 Identification and Disclosure Requirements

Pursuant to DFARS Subpart 211.106, contractors shall take all means necessary to not represent themselves as government employees. All contractor personnel shall follow the identification and disclosure requirement as specified in component clause - Contractor Identification. In addition, contractor and subcontractors shall identify themselves and their company name on attendance meeting list/minutes, documentation reviews, and their electronic digital signature.

4.4.2.6.3 Government Badge Requirements

As specified in component clause - Contractor Picture Badge, some contract personnel shall require a government issued picture badge. While on government installations/facilities, contractors shall abide by each site's security badge requirements. Various government installations are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards. Contractors are responsible for obtaining and complying with the latest security identification requirements for their personnel. Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, and/or SF-86 for Common Access Card (CAC)) to the applicable government security office via the contract COR. The contractor FSO shall track all personnel holding local government badges at contract or TO level.

4.5 IT POSITION CATEGORIES

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R, SECNAVINST 5510.30 and SECNAV M-5510.30, three basic DoN IT levels/Position categories exist:

- IT-I (Privileged access)
- IT-II (Limited Privileged, sensitive information)
- IT-III (Non-Privileged, no sensitive information)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The contractor PM shall assist the Government Project Manager or COR in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation

(SSBI-PR), and National Agency Check (NAC) adjudication will be performed Pursuant to DoDI 8500.01 and SECNAVINST 5510.30. IT Position Categories are determined based on the following criteria:

4.5.2 IT-I LEVEL (PRIVILEGED)

Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudication of Single Scope Background Investigation (SSBI) or SSBI-PR. The SSBI or SSBI-PR is updated a minimum of every 5 years. Assignment to designated IT-I positions requires U.S. citizenship unless a waiver request is approved by CNO.

4.5.2 IT-II Level (Limited Privileged)

Positions in which the incumbent is responsible for the-direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudication of a Position of Trust National Agency Check with Law and Credit (PT/NACLC). Assignment to designated IT-II positions requires U.S. citizenship unless a waiver request is approved by CNO.

4.5.3 IT-III Level (Non-privileged)

All other positions involved in computer activities. Incumbent in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudication of a Position of Trust National Agency Check with Written Inquiries (PT/NACI).

4.6 SECURITY TRAINING

Regardless of the contract security level required, the contractor shall be responsible for verifying applicable personnel (including subcontractors) receive all required training. At a minimum, the contractor FSO shall track the following information: security clearance information; dates possessing Common Access Cards; issued & expired dates; Cybersecurity training; Privacy Act training; Personally Identifiable Information (PII) training; Cybersecurity Workforce (CSWF) certifications; etc. The contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22-M.

4.6.1 DISCLOSURE OF INFORMATION

In support of DFARS clause, contractor employees shall not discuss or disclose any information provided to them in the performance of their duties to parties other than authorized Government and contractor personnel who have a "need to know". The contractor shall not use any information or documentation developed by the contractor under direction of the government for other purposes without the consent of the government Contracting Officer.

4.6.2 HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

When a contractor, including any subcontractor, is authorized access to Personally Identifiable Information (PII), the contractor shall complete annual PII training requirements and comply with all

privacy protections under the Privacy Act (FAR clause). The contractor shall safeguard PII from theft, loss, and compromise. The contractor shall transmit and dispose of PII in accordance with the latest DON policies. The contractor shall not store any government PII on their personal computers. The contractor shall mark all developed documentation containing PII information accordingly in either the header or footer of the document: "FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both criminal and civil penalties." Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer and COR. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel.

4.7 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

OPSEC is a five-step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or CPI, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

Applicable documents are as follows OPNAVINST F3300.53C (Series), Navy Antiterrorism Program, National Security Decision Directive 298 (Series), National Operations Security Program (NSDD) 298, DOD 5205.02 (Series), DOD Operations Security (OPSEC) Program, OPNAVINST 3432.1 (Series), and DON Operations Security.

4.7.1 OPSEC TRAINING

Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. Training may be provided by the government or a contractor's OPSEC Manager. Contractor training shall, as a minimum, cover OPSEC as it relates to contract work, discuss the Critical Information applicable in the contract/order, and review OPSEC requirements if working at a government facility.

4.7.2 CLASSIFIED CONTRACTS

OPSEC requirements identified under a classified contract shall have specific OPSEC requirements listed on the DD Form 254.

4.8 DATA HANDLING AND USER CONTROLS

4.8.1 DATA HANDLING

At a minimum, the contractor shall handle all data received or generated under this contract as For Official Use Only (FOUO) material. The contractor shall handle all classified information received or generated Pursuant to the attached DD Form 254 and be in compliance with all applicable PWS references and other applicable Government policies and procedures that include DOD and Navy.

4.8.2 EFFECTIVE USE OF CONTROLS

The contractor shall screen all electronic deliverables or electronically provided information for

malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect contract related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The contractor shall ensure provisions are in place that will safeguard all aspects of information operations pertaining to this contract in compliance with all applicable PWS references. The contractor shall ensure Data-at-Rest is required on all portable electronic devices including storage of all types. Encryption/digital signing of communications is required for authentication and non-repudiation.

4.9 GOVERNMENT FACILITIES

Government facilities (i.e., office space, computer hardware/software, or lab space) will be provided to those labor categories that would otherwise adversely affect the work performance if they were not available on-site.

Contractor personnel shall take all required training, which includes active shooter training, due to working space being located within a government facility.

4.10 CONTRACTOR FACILITIES

The Contractor shall provide the following at a minimum at time of award:

Access to an approved engineering & logistics facility. The facility will include at a minimum of 5,000 SqFt of certified Secure Storage Area (SSA), IAW Intelligence Community Directive (ICD) 705, Intelligence Community Standard (ICS) 705-1, Intelligence Community Standard (ICS) 705-2, and Intelligence Community Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities Version 1.3, for testing and storage of Contractor and Government procured installation equipment and material.

A minimum of 5,000 SqFt of warehouse storage and staging. for testing and storage of Contractor and Government procured equipment and material.

Access to conference rooms and meeting areas in Contractor facility with access to speakerphones, presentation systems, projectors, whiteboards, etc. necessary to support project meetings as needed. The facility must be within 20 miles of the NAS Oceana Dam Neck Annex, Virginia Beach, Virginia.

The facilities do not need to be dedicated and can be used to support other activities.

4.11 SAFETY ISSUES

4.11.1 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to the respective

Projects under this contract. Without government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system.

4.11.2 PERFORMANCE AT GOVERNMENT FACILITIES

In addition to complying with component clause - Occupational Safety and Health Requirements, the contractor shall immediately report any accidents involving government or contractor personnel injuries or property/equipment damage to the contracting officer and COR. Additionally, the contractor is responsible for securing the scene and impounding evidence/wreckage until released by the contracting officer.

4.11.3 SAFETY EQUIPMENT

The contractor shall provide their personnel with any safety equipment required to perform work under this contract and the equipment must be in satisfactory working order. Personal safety equipment includes, but not be limited to -- hard-hats, safety shoes, safety gloves, goggles, hearing protection, non-flammable clothing for hot work personnel, gas/oxygen detectors for confined spaces, face shields, and other types of safety equipment required to assure a safe work environment and compliance with applicable federal, state and local safety regulations.

4.11.4 SAFETY TRAINING

The contractor shall be responsible to train all personnel that require safety training. Specifically, where contractors are performing work at Navy shore installations, that requires entering manholes or underground services utility the contractor shall provide a qualified person as applicable in 29 CFR 1910 or 29 CFR 1926 or as recommended by the National Institute for Occupational Safety and Health (NIOSH) Criteria Document for Confined Spaces. Also, when contractors are required to scale a tower, all applicable personnel shall have Secondary Fall Protection and Prevention training.

4.12 TRAVEL

4.12.1 LOCATIONS

The contractor shall ensure all travel is performed pursuant to component clause - Reimbursement of Travel Costs. If travel is required at the order level, the contractor shall be prepared to travel, at a minimum, to the following locations:

- 1) DoD facilities worldwide (CONUS and OCONUS)
- 2) Others to be added

4.12.2 PERSONNEL MEDICAL REQUIREMENTS

4.12.2.1 OCONUS IMMUNIZATION REQUIREMENTS

As specified, the contractor shall be required to travel to locations outside the Continental limits of the United States (OCONUS) both shore and afloat. Contractor employees who deploy to locations that require immunizations shall do so pursuant to DoDI 6205.4 and Department of the Navy (DON).

4.12.2 LETTER OF AUTHORIZATION

Some travel will require a Letter of Authorization (LOA). As noted in DFARS PGI 225.7402-3(e), a LOA is necessary to enable a contractor employee to process through a deployment processing center; to travel to, from, and within a theater of operations; and to identify any additional authorizations and privileges. Applicable to the Project, the contractor shall initiate a LOA for each prospective traveler. The contractor shall use the Synchronized Pre-deployment & Operational Tracker (SPOT) web-based system, at <http://www.dod.mil/bta/products/spot.html>, to enter and maintain data with respect to traveling/deployed personnel, and to generate LOAs. When necessary and if in the Government's interest, the contractor may also initiate a LOA request to provide an official traveler access to Government facilities and to take advantage of travel discount rates in accordance with Government contracts and/or agreements. All privileges, services, and travel rate discount access are subject to availability and vendor acceptance. LOAs are required to be signed/approved by the SPOT registered Contracting/Ordering Officer for the applicable contract/order.

4.12.3 SPECIFIED MISSION DESTINATIONS

Pursuant to DoDI 3020.41 work to be performed at Specified Mission Destinations is subject to all relevant contract clauses, as well as the requirements set forth in the aforementioned guide. The contractor shall be able to meet all clause and guide requirements 35 days prior to travel within the applicable specified destinations. When deployment to a Specified Mission Destination is required, the contractor shall be responsible for processing applicable deployment packages for its personnel. The contractor shall be responsible to know and understand travel requirements as identified by the Combatant Command (COCOM) and applicable country. Commencing no later than seven (7) days after requiring travel to specified mission destination(s), the contractor shall submit all required OCONUS Deployment Documentation and Package to the Project technical POC and/or Command Travel/Deployment Coordinator.

4.12.4 CONTRACTOR SUPPORTING FORCES DEPLOYED

Pursuant to DFARS Subpart 225.371-5, if a contractor shall provide support to deployed forces, certain DoD class deviations exists dependent on the area of responsibilities (AOR): in particular CENTCOM, USSOUTHCOM, and AFRICOM. Contractor shall ensure compliance with applicable clauses as cited in the PWS.

SECTION 5.0 - DELIVERIES OR PERFORMANCE

5.1 PERIOD OF PERFORMANCE

The period of performance shall be for a base period of 12 months.

The period of performance table is below (subject to change based on actual award date):

Base Period:	September 2020 – September 2021
Option Period 1:	September 2021 – September 2022
Option Period 2:	September 2022 – September 2023
Option Period 3:	September 2023 – September 2024
Option Period 4:	September 2024 – September 2025

5.2 PLACE OF PERFORMANCE

The primary place of performance for the services is in a Government provided facility. Work may be extended to other locations within the United States or outside of the United States at the convenience of the government.

5.3 REPORT(S)/DELIVERABLES AND DELIVERY SCHEDULE

The contractor shall submit all required report(s)/deliverables in accordance with the following schedule: All reports shall reference and cite the contract number.

5.3.1 CONTRACT DATA REQUIREMENTS LIST (CDRLs)

The following listing identifies the data item deliverables required under this contract/TO. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs generated under each order. The contractor shall not develop any CDRL classified TOP SECRET with SCI.

CDRL#	Description	Classification	Frequency	Submit to
A001	Management Report, General, DI-MGMT-81797	UNCLAS	Periodically as required, due 10 days after CO written notification of revision requirement	CO & COR
A002	Monthly Status Report (MSR), DI-MGMT-80368A	UNCLAS	Submitted monthly, on the 20h of each month	CO & COR
A003	Data Call -	CLAS	Submitted as required;	TPOC as

	Technical/Analysis Reports, General, DI-MISC-80508B		delivered within forty-eight working hours of request unless otherwise specified	required
A004	Engineering Design Documents, General	CLAS	Submitted as required	TPOC as required
A005	Installation/As-built Drawings	CLAS	Submitted as required	TPOC as required
A006	Test/Inspection Report	CLAS	Submitted as required	TPOC as required
A007	Order Closeout Report	UNCLAS	15 days before the contract completion date	CO & COR, PM or as required
A008	RESERVED			
A009	RESERVED			
A010	RESERVED			
A011	Contract Funds Status Report (CFSR)	CLAS	10 business days after contract award	TPOC as required
A012	RESERVED			
A013	Cost and Schedule Milestone Plan	UNCLAS	With the Monthly Progress Report	CO & COR
A014	RESERVED			
A015	RESERVED			
A016	Trip/Travel Report	CLAS	5 Business Days after completion	TPOC as required
A017	Report, Record of Meeting/Minutes	UNCLAS	5 Business Days after completion	TPOC as required
A018				
A019	Warranty Tracking and Administration for Serialized Item Report	CLAS	Periodically as required	TPOC as required
A020	RESERVED			
A021	Training Documentation	UNCLAS	Periodically as required	CO & COR, PM or as required
A022	Monthly Changes to Performance & Quality Management Plan	UNCLAS	With the Monthly Progress Report	CO & COR
A023	Contract Funds Status Report (CFSR)	UNCLAS	With the Monthly Progress Report	CO & COR
A024	Quality Documentation	UNCLAS	With the Monthly Progress Report	CO & COR
A025	Cost and Schedule Milestone Plan	UNCLAS	With the Monthly Progress Report	CO & COR
A026	OCONUS Deployment Documentation and Package	UNCLAS	Periodically as required	CO & COR, PM or as required

5.3.2 ELECTRONIC FORMAT

At a minimum, the contractor shall provide deliverables electronically by e-mail; hard copies are only required if requested by the government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, etc., are provided in a format approved by the receiving government representative. *The initial or future upgrades costs of the listed computer programs are not chargeable as a direct cost to the Government.*

	Deliverable	Software to be used
a.	Word Processing	Microsoft Word
b.	Technical Publishing	PageMaker/Interleaf/SGML/ MSPublisher
c.	Spreadsheet/Graphics	Microsoft Excel
d.	Presentations	Microsoft PowerPoint
e.	2-D Drawings/ Graphics/Schematics (new data products)	Vector (CGM/SVG)
f.	2-D Drawings/ Graphics/Schematics (existing data products)	Raster (CALs Type I, TIFF/BMP, JPEG, PNG)
g.	Scheduling	Microsoft Project
h.	Computer Aid Design (CAD) Drawings	AutoCAD/Visio/Revit
i.	Geographic Information System (GIS)	ArcInfo/ArcView

5.4 DELIVERY REQUIREMENTS

Pickup and delivery of items shall be accomplished between the hours of 7:30 a.m. and 5:30 p.m., Monday through Friday unless changed by mutual agreement between the COR and the contractor. No deliveries shall be made on Saturdays, Sundays, and days of government closure or Federal legal holidays found at: http://www.opm.gov/operating_status_schedules.

5.5 OBSERVANCE OF LEGAL HOLIDAYS AND DAYS OF GOVERNMENT CLOSURE – ONSITE CONTRACTOR EMPLOYEES

(a)(1) Performance requires contractor employees of the prime contractor or any subcontractor, affiliate, partner, joint venture, or team member with which the contractor is associated, including consultants engaged by any of these entities, to have access to, physical entry into, and to the extent authorized, mobility within, a Federal facility.

(2) DoD entities may close and or deny contractor access to a Federal facility for a portion of a business day or longer due to any one of the following events:

(i) Federal public holidays for federal employees in accordance with 5 U.S.C. 6103.

(ii) Fires, floods, earthquakes, unusually severe weather to include snow storms, tornadoes and hurricanes.

(iii) Occupational safety or health hazards.

(iv) Any other reason.

(3) In such events, the contractor employees may be denied access to a Federal facility, in part or in whole, to perform work required by the contract. Contractor personnel already present at a Federal facility during such events may be required to leave the facility.

(b) In all instances where contractor employees are denied access or required to vacate a Federal facility, in part or in whole, the contractor shall be responsible to ensure contractor personnel working under the contract comply. If the circumstances permit, the contracting officer will provide direction to the contractor, which could include continuing on-site performance during the Federal facility closure period. In the absence of such direction, the contractor shall exercise sound judgment to minimize unnecessary contract costs and performance impacts by, for example, performing required work off-site if possible or reassigning personnel to other activities if appropriate.

(c) The contractor shall be responsible for monitoring when the Federal facility becomes accessible and shall resume contract performance as required by the contract.

(d) For the period that Federal facilities were not accessible to contractor employees, the contracting officer may—

(1) Adjust the contract performance or delivery schedule for a period equivalent to the period the Federal facility was not accessible;

(2) Forego the work;

(3) Reschedule the work by mutual agreement of the parties; or

(4) Consider properly documented requests for equitable adjustment, claim, or any other remedy pursuant to the terms and conditions of the contract.

SECTION 6.0 - SPECIAL CONTRACT REQUIREMENTS

6.1 KEY PERSONNEL

See 4.4.2.1.

6.2 PROHIBITION AGAINST PERSONAL SERVICES

The Contractor shall not perform personal services under this contract. Contractor personnel are employees of the Contractor or its subcontractors and are under the administrative control and supervision of the Contractor. A Contractor supervisor must give all individual Contractor employee assignments and daily work direction. The Government will not supervise or direct Contractor employees in the performance of their assignments. If at any time the Contractor believes that any Government action or communication has been given that would create a personal service relationship between the Government and any Contractor employee, the contractor shall promptly notify the Contracting Officer of this communication or action. The Contractor shall not perform any inherently-governmental functions under this contract. No Contractor employee shall represent or give the appearance that he/she is a Government employee, agent or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. The Contractor is responsible for ensuring that all employees assigned to this contract understand and are committed to following these requirements.

6.3 CONTRACTOR PERFORMANCE EVALUATION(S)

During the life of this Order, Contractor performance will be evaluated on an interim and final basis pursuant to FAR Subpart 42.15. The Contractor Performance Assessment Reporting System (CPARS) will be utilized for these reviews. Information on CPARS can be located at <http://www.cpars.gov>.

6.4 POST AWARD ORGANIZATIONAL CONFLICT OF INTEREST

(a) *General.* The Contractor shall have programs in place to identify, report, and mitigate actual and potential conflicts of interest for itself, its employees, subcontractors and consultants. The existence of such programs and the disclosure of known actual or potential conflicts are material performance requirements of this contract.

(b) *Disclosure.* The Contractor shall report all actual and potential conflicts of interest pertaining to this contract to the Contracting Officer, including those that would be caused by a contemplated modification to this contract or another contract. Such reports shall be in writing (including by email). Upon request, the Contractor shall respond to a Contracting Officer's request for an OCI mitigation plan.

(c) *Resolution.* In the event the Contracting Officer determines that a conflict of interest exists, based on disclosure from the Contractor or from other sources, the Contracting Officer shall take action which may include, but is not limited to, requesting a mitigation plan from the Contractor, terminating part or all of the contract, modifying the contract or obtaining a waiver in accordance with applicable law, including FAR 9.503 as applicable.

6.5 APPLICABLE DOCUMENTS

The following documents are mandatory for use. Unless otherwise specified, the document's effective date of issue is the date on the request for proposal.

	Document Number	Title
a.	DoD 5200.2-R	DoD Regulation – Personnel Security Program
b.	DoD 5220.22-M	DoD Manual – National Industry Security Program Operating Manual (NISPO)
d.	DoDD 8500.1	DoD Directive – IA
e.	DoDI 8500.2	DoD Instruction – IA Implementation
f.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT)
g.	DoDD 8570.01	DoD Directive – IA Training, Certification, and Workforce Management
h.	DoD 8570.01-M	IA Workforce Improvement Program
i.	SECNAVINST 5239.3B	DoN IA Policy
j.	SECNAVINST 5510.30	DoN Regulation – Personnel Security Program

The following documents are to be used as guidance. Unless otherwise specified, the document's effective date of issue is the date on the request for proposal.

	Document Number	Title
a.	MIL-M-85337A	Manuals, Technical; Quality Assurance Program: Requirements for

b.	MIL-DTL-24784	Manuals, Technical: General Acquisition and Development Requirements
c.	MIL-HDBK-61A	Configuration Management
d.	MIL-HDBK-881A	Work Breakdown Structure
f.	ISO/IEC -9000	International Organization for Standardization, Quality Management Principles
g.	ISO/IEC 12207	IT – Software Life Cycle Processes (provides common framework for developing and managing software)
h.	ISO/IEC 15288	Systems Engineering – System Life Cycle Processes
i.	ISO/IEC 15939	Software Engineering – Software Measurement Process
j.	ISO/IEC 14764	IT – Software Maintenance
k.	IEEE Std 12207-2008	Systems and Software Engineering – Software Life Cycle Processes
l.	IEEE/EIA 12207.1-1997	Guide for ISO/IEC 12207, Standard for IT – Software Life Cycle Processes – Life cycle data
n.	OSHA Standards	Occupational Safety and Health Act (OSHA) Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore)
o.	HPSD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
p.	NSA IA Technical Framework (IATF)	National Security Agency IA Framework
q.	DoDI 6205.4	Department of Defense Instruction, Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense
r.	DoD DTM-08-003	DoD Directive-Type Memorandum 08-003 – Next Generation Common Access Card (CAC) Implementation Guidance, December 1, 2008
s.	FIPS PUB 201-1	Federal Information Processing Standards Publication 201-1 – Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
t.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification
w.	MIL-STD-188, Series 100, 200, 300	DoD Standards, Defense Communications System
x.	MIL-HDBK-419A	DoD Handbook, Grounding, Bounding, and Shielding for Electronic Equipment and Facilities

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO., Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents

should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, VA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization's website.